I CLAIM:

1. A method for enabling secure communications among processing devices, comprising the steps of:

establishing a first cryptographically secure session between a first processing device and a second processing device, where said first processing device is remotely located from said second processing device;

establishing a second cryptographically secure session between a third processing device and a fourth processing device, where said third processing device is remotely located from said fourth processing device, where said first processing device communicates with said third processing device over a first communications link, and where said second processing device communicates with said fourth processing device over a second communications link;

generating a session key;

storing said session key in said first processing device;

sending session key information stored in said second processing device to said third processing device via said second communications link and said second cryptographically secure session;

generating said session key in said third processing device at least in part from said session key information;

storing said session key in said third processing device; and

establishing a third cryptographically secure session between said first processing device and said third processing device using said session key.

2. The method of claim 1 wherein said:

session key information comprises a second random number and where said step of generating a session key includes the substeps of:

said first processing device generating a first random number;

said second processing device generating said second random number and sending said second random number to said first processing device via said first cryptographically secure session; and

said first processing device forming said session key by exclusive ORing said first and second random numbers.

3. The method of claim 2 further comprising the steps of:

said first processing device sending said first random number to said third processing device via said first communications link; and

establishing the presence of said session key in said third processing device by exclusive-ORing said first random number and said second random number.

4. The method of claim 3 further comprising the steps of:

said first processing device sending said first random number to said second processing device via said first cryptographically secure session;

said second processing device forming said session key by exclusive ORing said first random number and said second random number;

said second processing device storing said session key;

said second processing device sending said second random number to said fourth processing device via said second communications link;

said first processing device sending said first random number to said fourth processing device via said first communications link and said second cryptographically secure session;

said fourth processing device forming a session key by exclusive ORing said first and second random numbers;

storing said session key in said fourth processing device; and

establishing a fourth cryptographically secure session between said second and fourth processing devices using said session key.

5. The method of claim 1, wherein information passing through said second cryptographically secure session is further encrypted by said first cryptographically secure session.

6. The method of claim 1, wherein said processing devices are tamper-proof.

7. The method of claim 6, wherein said first and second processing devices are trusted agents and said third and fourth processing devices are money modules.

8. A method for enabling secure communications among processing devices, comprising the steps of:

establishing a first cryptographically secure session between a first processing device and a second processing device, where said first processing device is remotely located from said second processing device;

establishing a second cryptographically secure session between a third processing device and a fourth processing device, where said third processing device is remotely located from said fourth processing device, where said first processing device communicates with said third processing device over a first communications link, and where said second processing device communicates with said fourth processing device over a second communications link;

said first processing device generating a first random number;

sending said first random number to said second processing device via said first cryptographically secure session and to said fourth processing device via said second communications link, whereby said first, second, and fourth processing devices store said first random number;

said second processing device generating a second random number;

sending said second random number to said first processing device via said first cryptographically secure session and to said third processing device via said first communications link, whereby said second, first, and third processing devices store said second random number;

said fourth processing device sending said first random number to said third processing device via said second cryptographically secure session;

said third processing device sending said second random number to said fourth processing device via said second cryptographically secure session;

said first processing device forming a random session key from said first and second random numbers;

said second processing device forming said random session key from said first and second random numbers;

said third processing device forming said random session key from said first and second random numbers;

said fourth processing device forming said random session key from said first and second random numbers; and

where said first and third processing devices cryptographically communicate with said session key, and where said second and fourth processing devices cryptographically communicate with said session key.

9. The method of claim 8, wherein information passing through said second cryptographically secure session is further encrypted by said first cryptographically secure session.

10. The method of claim 8, wherein said processing devices are tamper-proof.

11. The method of claim 10, wherein said first and second processing devices are trusted agents and said third and fourth processing devices are money modules.

Add A3 >

Add D3 >